MEIDI VAN DER LEE, *Cybersecurity Researcher, Edith Cowan University*
LinkedIn: https://www.linkedin.com/in/meidiz

Meidi is an experienced leader with a background in accounting, finance, company management, and governance. Whilst understanding the role of governance, risk management, and compliance (GRC) in safeguarding a company's assets and reputation, Meidi is attuned to the growing prevalence of cybersecurity threats. She conducts research in GRC and is a passionate advocate for leveraging these practices to strengthen a company's security posture.

TIP 1. PASSPHRASE IT AND USE 2FA / MFA

You hear it over and over again: use long passwords that combine letters, numbers, and symbols. But it's hard to remember complicated passwords. Instead, use words or phrases with symbols in place of spaces. Capitalise some letters and add numbers. This type of password is called a passphrase. If the login allows for two-factor authentication (2FA) or multi-factor authentication (MFA), use it. Activate this feature and follow the prompts.

TIP 2. CHANGE DEFAULT PASSWORDS

Did your smart printer come with a default password? Change it as soon as you set it up. The same goes for all IoT devices (the smart appliances that connect to your Wi-Fi), including your coffee machine and smart TV. These devices should be connected to a separate Wi-Fi channel configured for IoT, not the one used for work computers. Some routers come with pre-configured, secure channels for IoT devices.

TIP 3. WHEN FINANCIAL DATA IS INCLUDED, DOUBLE CHECK, TRIPLE CHECK, OUT OF BAND CHECK

Received a billing invoice with a bank account for payment? Double-check it against your previous records. Triple-check with the supplier. Verify an email with a fax or phone call. Confirm a phone call with an email or text message. Sometimes, direct, real-life communication with the supplier's office might be necessary. Always verify sensitive information using a different channel from the one in which the message was originally received.

TIP 4. PHISHING COMES IN MANY WAYS – DO NOT CLICK!!

Anything that lures you with false pretences is a phishing attempt. If it comes via email, text message, or social media, do not click any links or open any attachments. Delete the message and report it as spam if that option is available. If the phishing attempt comes as a voice call, be cautious and do not give away any personal information, passwords, PIN numbers, or OTPs

TIP 5. PRIVACY IS A COMMODITY – PROTECT IT LIKE YOU PROTECT YOUR INVENTORY

Privacy-related data, also known as personally identifiable information (PII), can be used to impersonate or scam the data owner. Hackers steal this data and sell it on the dark web. You are responsible for the privacy data you collect from your employees, contractors, customers, and yourself. Secure the storage of this data. Activate the highest level of encryption on your electronic storage. Enhance the security of your physical storage.

TIP 6. OPERATING SYSTEM AND APPLICATION UPDATES

Updates may seem to take up productive time, but it is highly recommended to install them as soon as possible. System and application vendors usually push updates that improve security, in addition to enhancing functionality and features. This recommendation applies to all devices, including computers, tablets, and Smartphones. Make sure to only update through the system manufacturer's official channels.

TIP 7. BACKUP... BACKUP... BACKUP...

Back up all your data and back up the backup. Combine cloud backup with external storage or use multiple cloud services. Ensure your backups are restorable. For hardcopy or external storage backups, ensure their physical security and safe keeping. In the event of disruption, your backup is your lifeline.

TIP 8. SECURE YOUR WIFI AND SEGREGATE ACCESS

Use a WiFi router that supports the latest security standard, WPA3. Set a strong passphrase for Wi-Fi access. Create guest channels if you need to allow outsiders to connect. Also, create segregated channels for IoT devices. Some routers come with pre-configured channel segregation, but it is a good idea to review the default settings.

TIP 9. BUILD SECURITY CULTURE IN THE TEAM

Talk about cybersecurity. Train your team to recognise secure and insecure cyber behaviour. Start with common sense practices and build towards greater resilience against cyber threats. Encourage team members to report unusual or suspicious cyber activities; including if someone has clicked on a phishing link. One person may be the weakest link, but together, the team can be resilient.

TIP 10. PLAN B IN CASE OF SYSTEM FAILURE

If you or your company fall victim to a scam, what's next? Do you know where to get help? Do you know where to report the incident? Do you have a step-by-step plan to recover your business? Is this information readily available in a crisis? Even without a hacker, IT systems can fail for various reasons. A business continuity plan is a must-have.